ISSN 2358-6036
v.9 2021
RevInt
Revista Interdisciplinar de Ensino, Pesquisa e Extensão
UNICRUZ

ATAQUES CIBERNÉTICOS USANDO ENGENHARIA SOCIAL

Cyber attacks using social engineering

Daniel de Moura Dorneles[1]
Rafael Barasuol Rohden[2]
Alex Vinicios Telocken[3]

Resumo: Ataques que focam a obtenção de fatos pessoais, senhas ou qualquer outro dado que que pode ser considerado sensível, ocorrem desde muito tempo antes da existência de máquinas. Enganar, ludibriar e extorquir uma pessoa para que ela lhe forneça dados importantes da sua vida social ou privada e até mesmo de seus familiares, pode ser um obstáculo para atacantes quando a vítima possui algum conhecimento do certo ou errado dentro ou fora da internet. Como a internet se tornou um meio de comunicação global e fácil de se tornar anônimo, é um local propicio para que vazamento de dados ocorra, portanto, medidas devem ser tomadas ao utilizar desta ferramenta.

Palavras-chave: Internet. Ataque. Vítima.

Abstract: Attacks that focus on obtaining personal facts, passwords or any other data that might be considered sensitive, have been taking place long before the existence of machines. Deceiving, deceiving and extorting a person to provide important information about their social or private life and even their family members, can be an obstacle for attackers when the victim has some knowledge of right or wrong on or off the internet. As the internet has become a global means of communication and it is easy to become anonymous, it is a favorable place for data leakage to occur, therefore, measures must be taken when using this tool.

Keywords: Internet. Attack. Victim.

1 INTRODUÇÃO

A falta de cuidados com segurança por parte das empresas ou até mesmo usuarios comuns por trás desses ataques. “Isso [vazamento de dados] passa muitas vezes pela falta de atualização de um software, falta de incorporação de novas tecnologias, de novos métodos para evitar que esse tipo de situação aconteça”, afirma Tiago Antônio Rizzetti, professor do curso de Tecnologia em Redes de Computadores do Colégio Técnico Industrial de Santa Maria (CTISM). Manter-se bem atualizado, seja socialmente, descobrindo os novos tipos de ataques, vivenciando depoimentos e orientações das autoridades ou computacionalmente, na atualização do sistema operacional instalado em sua maquina e anti-virus, é essencial para que

[1] Discente do curso de Ciência da Computação. Universidade de Cruz Alta - Unicruz, Cruz Alta, Brasil. E-mail: danielm.dorneles@gmail.com

[2] Docente da Universidade de Cruz Alta - Unicruz, Cruz Alta, Brasil. E-mail: rafbarasuol@unicruz.edu.br

[3] Docente da Universidade de Cruz Alta - Unicruz, Cruz Alta, Brasil. E-mail: telockenalex@unicruz.edu.br.

ataques de sequestro de dados possam ser evitados. De acordo com a BBC, “Especialistas em segurança dizem que a chave para evitar essas armadilhas é lembrar que nenhum banco, agência estatal ou instituto de saúde entra em contato com solicitando informações confidenciais.

1.1 Internet

No Brasil, a primeira aplicação da Internet ocorreu em 1988 sendo usado apenas para conectar centros de pesquisa do Brasil aos da América do Norte, e as primeiras universidades no Brasil a usar a rede foram USP, Unicamp e PUC que só foi possível devido ao primeiro teste de conexão de rede realizado pela Rede Nacional de Ensino e Pesquisa (RNP), que já em 1992, começou a desenvolver AlterNex, uma rede não governamental e não acadêmica de compartilhamento, em outras palavras, para uso comercial que depois de muitos testes, o Ministério da Educação e o Ministério da Ciência e Tecnologia assinaram um acordo em 1999 para fornecer a Internet em todo o país, assim implementando efetivamente a Internet (Zoom).

Grosso modo, a internet nada mais é que uma enorme rede de compartilhamento de dados, conhecida por ser um sistema global de redes de computadores interligados, ou seja, você poderia iniciar uma conversa em poucos segundos com outro usuário que se encontra do outro lado do planeta terra, ou até mesmo fora dele, dependendo do método de comunicação utilizada, como descreve Rodrigo Lara, colaborador da Tilt UOL. Desta forma, até mesmo um astronauta pode sim cair em um golpe, dentro ou fora da terra, por estar conectado aos mesmos protocolos de compartilhamento.

1.2 Phishing

Também conhecido como Scam/Phishing, foi originalmente concebido para descrever os tipos de fraude que ocorrem ao enviar mensagens não solicitadas que são entregues por meio de comunicações de bancos, empresas populares ou organizações em sites. Também tenta induzir o acesso a páginas fraudulentas (forjadas) com o objetivo de roubar dados pessoais e financeiros dos usuários.

O termo phishing (de "fishing") vem de uma analogia aos fraudadores, em que "isca" (e-mail) é usado para "pescar" senhas e dados financeiros de usuários da Internet (Informática para Concursos, 1ª Edição - Samuel Liló Abdalla).

O phishing usa e-mails de supostas instituições financeiras (eBay, PayPal, Bancos Digitais) para indicar que há um problema com a conta e o titular da conta precisa fazer login para configurá-la corretamente. O proprietário recebe um link e, se usado, será direcionado para um site que é claramente idêntico ao site da empresa real. Quando o titular faz login, o golpista irá capturar seu nome de usuário e senha (Segurança de Computadores e teste de invasão - Tradução da 2ª edição norte-americana - Alfred Basta).

1.3 E-mail

A maioria dos usuários de computador hoje já sabe que anexos de e-mail podem conter vírus e Worms (vermes que infectam a máquina). Este fato é conhecido há muito tempo, de modo que algumas pessoas nem mesmo abrem nenhum tipo de anexo. O worm pode enviar e-mails para o próprio usuário e para todos os endereços de seu catálogo de endereços, fazendo o destinatário acreditar que o e-mail é do usuário-alvo do ataque. Os emails enviados por worms geralmente são mal escritos e os destinatários cuidadosos certamente perceberão que esses e-mails não são normais.

De qualquer forma, algumas pessoas acabaram de abrir o anexo e não sabem o que contém além de fotos de férias ou arquivos de trabalho. Se a infeliz vítima usar o sistema operacional para qual o verme foi criado, o malware será copiado rapidamente para todos os endereços de e-mail em seu catálogo de endereços e assim, disparando para todos eles automaticamente. Enquanto aqueles que não abrirem o anexo não serão infectados por vírus ou worms. Controles de segurança devem ser adotados como prática padrão. Algumas tecnologias de conexão remota permitem que os usuários ignorem os controles de rede típicos ao abrir seus e-mails privados (Segurança de Computadores e teste de invasão - Tradução da 2ª edição norte-americana - Alfred Basta).

1.4 Segurança da Informação

Como todo e qualquer dado é suscetível a modificação, existem pilares, como demonstrado na Figura 1, que delimitam a segurança da própria informação, existem alguns pilares que são essenciais na manutenção dos dados, que são eles, Disponibilidade, Confidencialidade, Integridade, assim como aponta os dados da G Data Security, possuidora de um dos antivírus mais famosos do mundo. Toda empresa que está online, está sob constante ameaça de qualquer vírus de computador e de usuários maliciosos, além disso a

empresa também aponta que um novo vírus de computador surge a cada três segundos (G DATA SECURITY, 2017)

Disponibilidade

Esse pilar refere-se à acessibilidade que se tem dos dados, as informações precisam estar disponíveis para que possam ser consultados a qualquer momento por quem possui as permissões de segurança, sendo então necessário trabalhar de forma síncrona com várias condições, entre elas os processos de manutenções dos servidores, atualizações constantes, e um dos fatores importantes a serem mencionados a alta disponibilidades de serviços e links de internet (G DATA SECURITY, 2017).

Confidencialidade

O pilar em questão, permanece diretamente ligado aos procedimentos e métodos que garantem o controle de acesso as informações sensíveis, dessa forma restringindo os dados a quem está autorizado, mas respeitando todos os pilares. Talvez um dos pilares mais importantes, pois através dele se assegura que as informações não sejam sequestradas por meio de ataques. (TECHTEM, 2019)

Integridade

Corresponde à preservação da precisão, consistência e confiabilidade das informações e sistemas pela empresa ao longo de seu ciclo de vida, sendo completamente importante que os dados circulem ou sejam armazenados do mesmo modo como foram criados, sem que haja interferência externa para corrompê-los, comprometê-los ou danificá-los. Assim, uma informação sem integridade gera prejuízo e trabalho dobrado, assim perdendo um precioso tempo dentro da empresa, o que é chamado de ineficiência (TECHTEM, 2019).

Com ciberataques cada vez mais sofisticados, as empresas devem estar atentas para a adoção de soluções de segurança de modo a prevenir os perigos vindos da Internet e, com isso, proteger os pontos de extremidade da rede. Entende-se por pontos de extremidade todos os dispositivos nos quais o trabalho é realizado, ou seja, servidores, estações de trabalho e dispositivos móveis (TECHTEM, 2019).

Autenticidade

É garantia de que a informação vem de uma fonte confiável, dessa forma é possível confirmar sua autoria e originalidade afim de garantir a identidade de quem está enviando a informação (Segurança de Redes em Ambientes Cooperativos, 2007). Essa pesquisa em questão possui o intuito de auxiliar usuários que não tem o devido conhecimento e que está vulnerável a qualquer ataque, desde ataques em pequena escala até grandes invasões que

possam comprometer a empresa em que o usuário trabalha ou que comprometa a sua integridade.

Figura 1 - Pilares da Informação.

Fonte: UFRJ (2020).

Com ataques cibernéticos cada vez mais sofisticados, as empresas devem estar atentas para a adoção de soluções de segurança de modo a prevenir os perigos vindos da Internet e, com isso, proteger os pontos de extremidade da rede. Entende-se por pontos de extremidade todos os dispositivos nos quais o trabalho é realizado, ou seja, servidores, estações de trabalho e dispositivos móveis (PIO, 2021). Com isso leis foram implementadas ao código de lei brasileiro como a lei Carolina Dieckmann, para que em casos de crimes cibernéticos, não seja necessário adaptar leis como de estelionato ou usurpação.

1.5 Legislação

Todo e qualquer avanço desenfreado, requer normativas de uso, sob quaisquer circunstâncias, a internet não é uma exceção, principalmente quando se trata de dados pessoais, seja eles privados ou públicos, portanto, crimes cibernéticos no Brasil precisavam de

uma visibilidade, além de receber leis adaptadas, como: insultar a honra de alguém (calúnia artigo138), espalhar boatos eletrônicos sobre pessoas (difamação artigo 139), insultar pessoas considerando suas características ou utilizar apelidos grosseiros (injúria artigo 140), ameaçar alguém (ameaça artigo 147), utilizar dados da conta bancária de outrem para desvio ou saque de dinheiro (furto artigo 155), comentar, em chats, e-mails e outros, de forma negativa, sobre raças, religiões e etnias (preconceito ou discriminação artigo 20 da Lei n. 7.716 /89), enviar, trocar fotos de crianças nuas (pedofilia artigo 247 da Lei n. 8.069 /90, o Estatuto da Criança e do Adolescente - ECA).

Lei Carolina Dieckmann

A Lei Carolina Dickman é a Lei nº 12.737 / 2012, uma emenda ao Código Penal Brasileiro, com foco em crimes cibernéticos e crimes informáticos. Com o avanço e a democratização da tecnologia e a facilidade de acesso às redes sociais, o judiciário brasileiro acredita que é necessário tipificar os crimes cometidos em ambientes virtuais.

Seu projeto foi apresentado em 29 de novembro de 2011 e aprovado pela Presidente Dilma Rousseff em 2 de dezembro de 2012. Este é o primeiro texto típico de crime cibernético que enfoca invasões em dispositivos sem a permissão do proprietário (FMP RS).

O caso de Carolina que originou o crime e consequentemente mais tardem a sua lei, foi quando o hacker acessou seu computador pessoal por meio de um e-mail infectado no qual a atriz clicaria para obter fotos privadas da atriz, incluindo fotos nuas e fotos de família com seu filho de quatro anos. Inicialmente, pensou-se que a invasão poderia ter ocorrido em uma loja que consertava computadores na Carolina há alguns meses.

Logo depois, descobriu-se que hackers de Minas Gerais e de São Paulo cometeram o crime. A atriz foi chantageada por criminosos que exigiram o pagamento de 10 mil reais para impedir que as fotos aparecessem nas redes sociais (MENDES, 2012).

Uma vez que o Brasil não possui leis que visem especificamente os crimes de informática, os envolvidos serão acusados de furto, extorsão e difamação, todos pertencentes à legislação penal brasileira. Antes do caso da atriz, muitas vítimas haviam sido registradas, no entanto, o caso recebeu atenção como figura pública.

Esse é um caso típico de phishing (com a modalidade de e-mails de spam contendo links de sites falsos), que costumam trazer alguns “benefícios”, mas no final vão acabar capturando e danificando a integridade dos seus dados (MACHADO, 2017).

Independente da criação desta lei, os dados ainda permaneciam inseguros por não abrangerem todo um conjunto de normas específicas para o tratamento de todo e qualquer dado ou para o uso da internet, por conta disso a implementação da lei do Marco Civil da internet.

Marco Cívil da Internet

Inicialmente, pensava-se que a Internet poderia ser considerada uma "terra de ninguém" sem supervisão, visto que a informação ali era divulgada de forma descentralizada e fornecida pelos usuários de forma descontrolada.

Porém, a partir do momento em que se observa que o relacionamento na Internet tem impacto para além do mundo virtual, a fiscalização se faz necessária, e a lei não pode se furtar a essa responsabilidade. Um exemplo simples é a crescente ocorrência de relacionamentos com consumidores em ambientes virtuais por meio de muitas lojas de e-commerce existentes. Como todos sabemos, o estudo das leis e as leis aplicáveis em um determinado tempo e espaço não são impenetráveis. Devem atender às necessidades que surgem com o desenvolvimento da sociedade, seja no campo ético, relacionado aos costumes de cada época, seja relacionado ao avanço da tecnologia, como o surgimento do Marco Civil da Internet.

O que precisa ser esclarecido é que na Internet também é extremamente importante a aplicação dos princípios da racionalidade e da proporcionalidade. Isso porque há um claro conflito entre direitos como o direito de todos à privacidade e a liberdade de expressão, os dois direitos constitucionais estipulados no art. 5 Nos Artigos IX e X da Constituição Federal de 1988:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> IX – é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
> X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação."

Também dispondo acerca do princípio constitucional da privacidade, o art. 5, inciso XII:

> XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal."

Em termos de privacidade, o Marco Civil da Internet surgiu da necessidade de proteger dados pessoais indevidamente utilizados por terceiros, pois o fato de os dados serem exibidos

publicamente em meio digital ou encaminhados a terceiros não garante seu uso ou exibição não autorizados.

> art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II – proteção da privacidade."

É seguindo esse raciocínio, que o art. O artigo 7 da mesma lei estipula da os requisitos do usuário para a liberdade e consentimento explícito, bem como o direito à intimidade e inviolabilidade da vida privada.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I – Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei."

Este e um conjunto de leis agora tem um intuito de proteger o usuário quanto à tratativa de vazamento de dados, liberdade e uso da internet no geral, mas, para que os dados sejam tratados de sua forma original, quanto compartilhamento, vazamento e principalmente à padronização de como tratar dados de colaboradores, clientes ou qualquer um que esteja ligado a empresas, fora criado um conjunto de leis conhecido por Lei Geral de Proteção de Dados (LGPD).

LGPD

Alguns dias depois o grupo identificou que haviam realizado uma parceria com o grupo Anonymous, onde fora criado uma "Operação Anti-segurança", que realiza ataques em sites governamentais como resposta a esforços para "dominar e controlar nosso oceano da internet". Este ataque conhecido como "Grey Hat", tem a intenção de realizar a invasão deixando apenas danos leves, agindo como se fosse "brincadeira" e tem como foco demonstrar como as determinadas redes possuem uma vulnerabilidade muito alta. Atualmente existem alguns tipos de ataques, como o "Gray hat", sendo o Black Hat e o White Hat.

A partir do dia 14 de setembro de 2020, uma nova lei entra em vigor, a lei geral de proteção de dados, que estava em discussão desde 2014. A lei conta com diversas adequações onde a empresa dá o devido valor a todo e qualquer dado que a empresa possua, dando empoderamento ao usuário quanto a seus dados e protegendo toda informação, sendo ela de usuário cadastrado na empresa ou não, como mostra na Figura 2.

Figura 2 – LGPD.

Fonte: Protiviti (2020).

Em caso de não adequação às leis, a partir de 2021, haverá multa diária de até 2% do faturamento da empresa, limitado a 50 milhões, além da exclusão e bloqueio de dados que possam infringir algum artigo da lei, e em alguns casos até a proibição parcial ou total do exercício de atividades que estão vinculadas ao tratamento de dados, podemos observar no art. 52:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I - Advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;
>
> IV - Publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V - Bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI - Eliminação dos dados pessoais a que se refere a infração;
>
> X - Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019);
>
> XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019);
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019) .

A nova lei brasileira, baseada na legislação europeia, foi após ter sido colocada em vigor, dentro do mesmo mês foi utilizada em uma decisão judicial.

A juíza Tonia Yuka Koroku condenou a empresa imobiliária Cyrela por divulgar os dados de um cliente sem sua autorização, após ele comprar um apartamento. Depois da realização da compra, instituições financeiras e empresas de decoração começaram a perturbar a paz do cliente, oferecendo serviços não solicitados, e que citavam o conhecimento da recente aquisição, algo que só a imobiliária (além do próprio cliente) teria como informar.

Além da LGPD, a empresa condenada infringiu o Código de Defesa do Consumidor e artigos da Constituição Federal, sendo então condenada a pagamento de multa indenizatória de R$10.000,00 reais à vítima, durante o processo, a empresa acabou tentado processar o cliente por danos morais, acusação que a juíza achou improcedente.

Embora não pague o estresse sofrido pela vítima, além do transtorno de saber que dados pessoais podem ter sido compartilhados com outras empresas sem seu conhecimento e consentimento, a punição oferece uma compensação pela perturbação e punição a empresa infratora, para que a última talvez comece a repensar em sua política de compartilhamento de dados e evite que mais clientes passem pela mesma situação. (Fernanda Valente, 2019, conjur).

2 PROCEDIMENTOS METODOLÓGICOS

Para a realização deste trabalho, foram usados trabalhos, artigos e casos reais de aplicações das leis de proteção de dados e privacidade, classificamos esta pesquisa como um Estudo de Caso, que, segundo Branski (s.d), é uma pesquisa que utiliza, geralmente, dados qualitativos, coletados a partir de eventos reais, com o objetivo de explicar, explorar ou descrever fenômenos atuais inseridos em seu próprio contexto.

A Abordagem que esta pesquisa teve foi de enfoque qualitativa, por se especificar em um tema em específico e sua compreensão. Segundo Silveira (2009), a pesquisa qualitativa não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social, de uma organização etc.

Os objetivos têm como foco explicativo devido a sua explicação sobre as leis de proteção de dados e os resultados que ele trouxe com a sua implementação.

Os procedimentos adotados para a realização deste artigo foram bibliográficos devido ao levantamento de trabalhos, lei e estudos de caso que já aconteceram.

3 RESULTADOS E DISCUSSÃO

Como forma de demonstração de captura de dados, será realizado uma simulação em um ambiente isolado de como ocorre a captura de senhas através de uma clonagem de site, conhecida como Phishing.

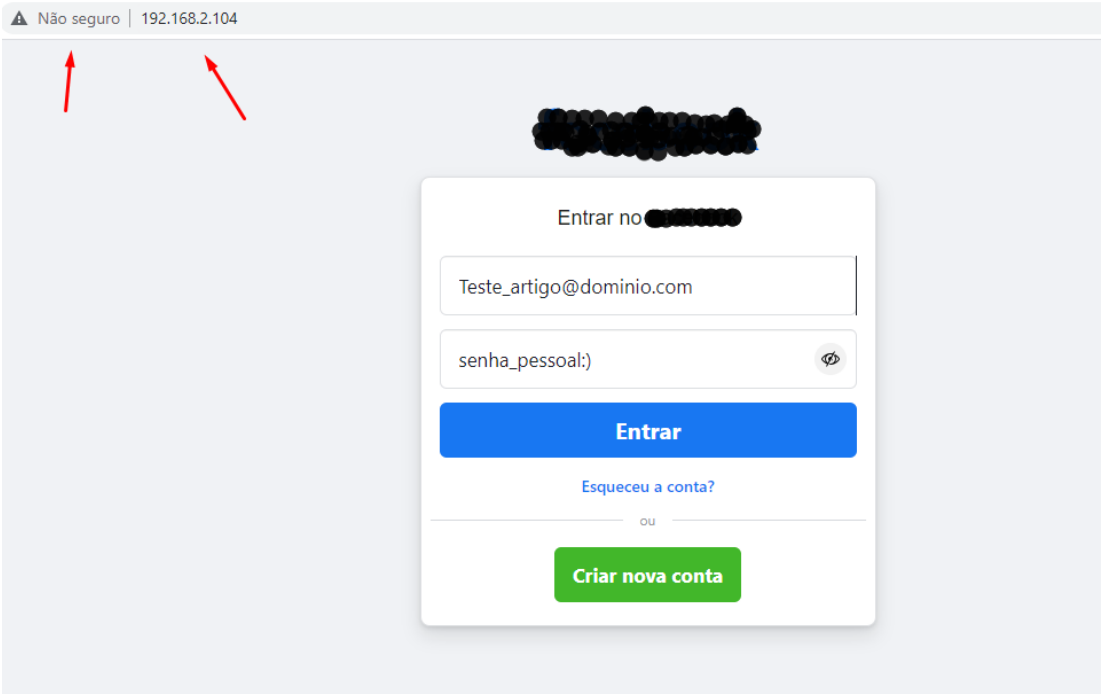
3.1 Objetivo

O objetivo deste trabalho é conscientizar pessoas sobre possíveis golpes na internet, e demonstrar como a evolução das leis impactaram no meio judicial, desta forma, tornando os pilares da segurança da informação cada vez mais sólidos dentro e fora de empresas.

3.2 Demonstração de Phishing

Para que se tenha uma noção de como é um ataque no formato Phishing de captura de senhas, será demonstrado como ocorre de forma local e isolado para demonstração acadêmica, não ferido lei alguma dentro da LGPD. O ataque se dá a partir da clonagem de um site, como demonstrado na Figura 3, a página é copiada em seu método de autenticação, seja ele de lojas online, banco, redes sociais ou qualquer que seja o site que possua um método de autenticação com ID e senha. Como a clonagem se da de forma local, o endereço URL do site é o IP da máquina que o está hosteando, sendo assim, não existindo contato com a rede externa.

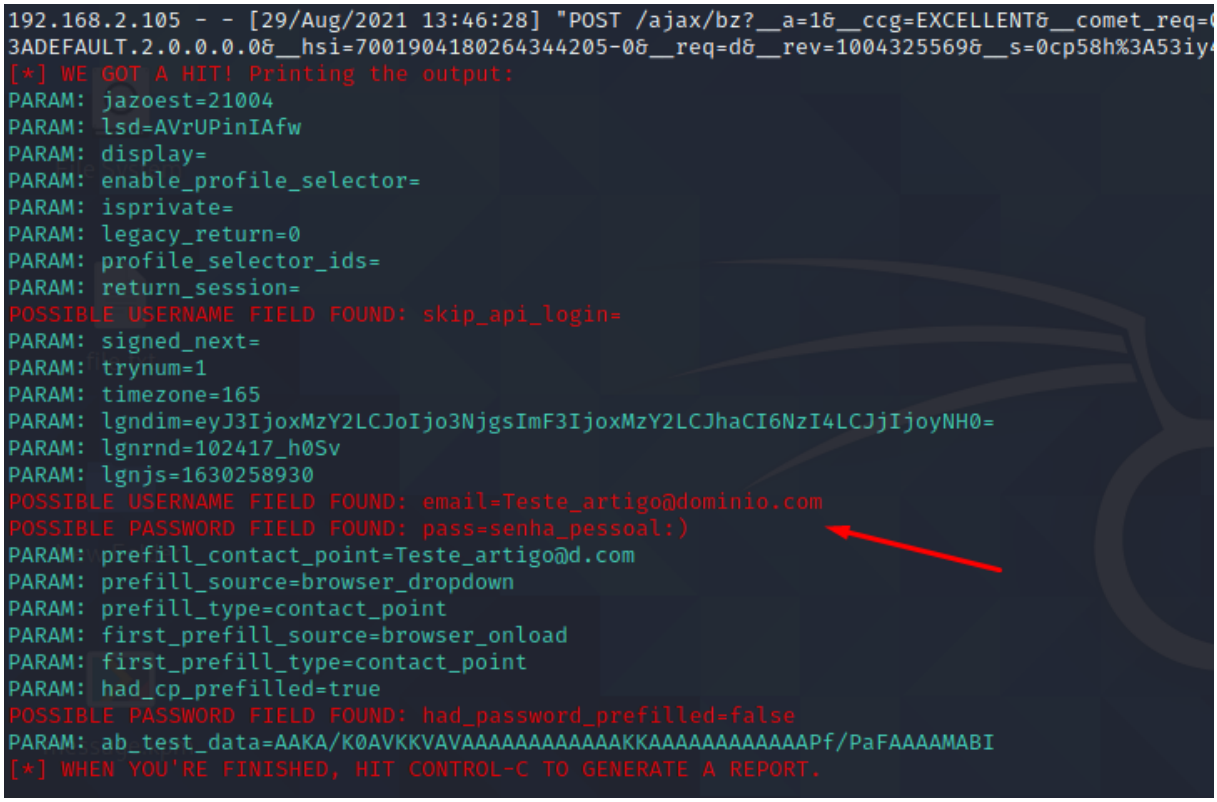
Figura 3 - Página clonada.



Fonte: Autores (2021).

Quando o usuario preenche com seus dados e clica no botão de ingressar, o site é redirecionado para o real endereço online, ingressando automaticamente em sua conta caso esteja correta, muitas vezes passando por despercebido pelo usuario enquanto o hacker conquista todos os dados preenchidos, como demonstado na Figura 4.

Figura 4 - Dados capturados.



Fonte: Autores (2021).

Desta forma, o usuario mal intencionado consegue coletar todo e qualquer dado escrito pelo usuario em sua pagina de autenticação reservada, portanto, deve-se sempre estar prestando atenção em links ou locais acessados, propagandas de produtos cujo o valor seja longe da realidade e até mesmo em mensagens SMS recebidas indicando compras exuberantes que não foram realizadas.

5 CONSIDERAÇÕES FINAIS

É necessário sempre verificar se estamos de acordo com a lei, não compartilhando dados sensíveis de terceiros ou de si próprio, para que não haja problemas com a tratativa dos dados. Quanto à links recebidos, compras indevidas registradas ou sites com preços muito

inferiores ao padrão, o primeiro passo ao registrar isso, é conversar diretamente com o suporte da empresa que oferece o serviço.

REFERÊNCIAS

ALENCAR, Morgana, UFP. **Tire as suas dúvidas sobre o Marco Civil da Internet.** 2021. Disponível em: https://www.aurum.com.br/blog/marco-civil-da-internet/. Acesso em: 29 ago. 2021.

BASTA, Alfred. **Segurança de Computadores e teste de invasão**. Tradução da 2ª edição norte-americana, TRILHA. (24 agosto 2014).

BBC News. **3 novos tipos de fraudes e golpes surgidos com a pandemia de covid**. 2009. Disponível em: https://www.bbc.com/portuguese/internacional-56034335. Acesso em: 29 ago. 2021.

BRANSKI, Regina Meyer, FRANCO, Raul Arellano Caldeira, LIMA, Orlando Fontes. **Metodologia de Estudo de Casos Aplicada à Logística. Artigo**, pg. 1. Campinas. Campus. s.d.

BRASIL. Presidência da República. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em:< http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 28 ago. 2020.

BRASIL. **Lei 13.709 de 14 de agosto de 2018**. Disponível em <http://www.planalto.gov.br>. Acesso em 20 nov. 2020.

DO NASCIMENTO, Janilson Pereira. Segurança em Redes de Computadores: Uma Abordagem sobre o Comprometimento Individual em Benefício da Corporação. **Tecnologias em Projeção**, v. 6, n. 1, p. 01-06, 2015.

FUNDAÇÃO ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO. **Lei Carolina Dieckmann: você sabe o que essa lei representa?** 2021. Disponível em: https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/. Acesso em: 29 ago. 2021.

GDATA Security. **Cybercrime,** 2021. Disponível em: < https://www.gdatasoftware.com/blog/cybercrime/>. Acesso em: 10 set. 2021.

LARA, Rodrigo. **Wi-fi espacial: como astronautas se conectam à internet fora da Terra?** 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/07/16/wi-fi-espacial-como-astronautas-se-conectam-a-internet-fora-da-terra.htm. Acesso em: 29 ago. 2021.

MACHADO, Tiago. **Cibercrime e o crime no mundo informático.** 2017. Disponível em: https://bdigital.ufp.pt/bitstream/10284/6089/1/DM_Thiago%20Machado.pdf. Acesso em: 29 ago. 2021.

MENDES, Maria Eugencia Gonçalves; VIEIRA, Natália Borges. **Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica**. 2012. Disponível em: <http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2>. Acesso em: 12 de ago. 2021.

NAKAMURA, Emilio; GEUS, Paulo Lício. **Segurança de Redes em Ambientes Cooperativos.** 1ª edição. Novatec (24 agosto 2007).

OLIVEIRA, Waldes. **Princípios Básicos Da Segurança Da Informação.** 2019. Disponível em: < https://www.techtem.com.br/principios-basicos-da-seguranca-da-informacao/ >. Acesso em: 10 set. 2020.

PIO, Vitor. **O que é um teste de intrusão e por que preciso dele?** 2021. Disponível em: https://www.sidi.org.br/o-que-e-um-teste-de-intrusao/>. Acesso em: 10 set. 2021.

REDAÇÃO ZOOM. **O que é internet? O que significa esse nome?** 2021. Disponível em: https://www.zoom.com.br/modem-e-roteador/deumzoom/o-que-e-internet. Acesso em: 29 ago. 2021.

SILVEIRA, Denise Tolfo. **Métodos de Pesquisa.** 2009. Disponível em: http://www.ufrgs.br/cursopgdr/downloadsSerie/derad005.pdf. Acesso em: 29 ago. 2021.

SILVEIRA, Neil; SOUSA, Mirian; ALCÂNTARA, Antônia. **Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann.** 2017. Disponível em: <https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann>. Acesso em: 29 de ago. 2021.